UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/597,003	07/06/2006	Gil Sever	P-9541-US	4617

49443 7590 06/25/2010
Pearl Cohen Zedek Latzer, LLP
1500 Broadway
12th Floor
New York, NY 10036

EXAMINER	
ANDERSON, MICHAEL D	

ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
06/25/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/597,003	**Applicant(s)** SEVER ET AL.	
	Examiner MICHAEL ANDERSON	**Art Unit** 2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 April 2010*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *4/15/2010*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement (IDS) submitted on 4/15/2010 was filed. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

2. Pending claims for reconsideration are **claims 1-37.** Applicant has amended claims 1-5, 9-21, 26, 28, 31, 32 and 34. Claims 36-37 have been added.

3. The Rejection of **Claim 1** and all intervening claims under 35 USC 101 as allegedly not falling within one of the four statutory categories of invention have been **withdrawn in light of applicants amendment to claim 1.**

4. The Rejection of **Claims 21** and all intervening claims under 35 USC 101 as allegedly not falling within one of the four statutory categories of invention have been **withdrawn in light of applicants amendment to claim 21.**

5. Applicant's arguments with respect to claims 1-37 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-20, 35, and 37** are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent No.: US 6,587,949 B1 to Steinberg, in view of Pub.No.: US 2002/0073340 A1 to Mambakkam et al (hereafter referenced as Mambakkam) in further view of Patent Number: 4,799,153 to Han et al (hereafter referenced as Hann).

Regarding **claim 1**, Steinberg discloses " A method for protecting the transfer of data between a computer and an external device"***(secure storage device interconnected to a to an external device with a security function/encryption [abstract])***, "the method comprising the steps of: a. receiving, by a module on the computer, a data portion during a data communication session between the computer and the external device", ***i.e. receiving data from external device to computer (computer receives data from the storage device [Col.5/line 33-35] also see [Fig.7] which illustrates host computers verification process of received data)*** , "said external device connected to the computer and communicating therewith via a physical communication port"***(compatible communication port[Fig.1/item 26])***, "the data portion being associated with a particular physical communication port of the computer and with the device that is currently communicating via the particular physical communication port"***(data is associated with device via a program that allows data to be transferred and stored from camera to device and to computer[Col3/line 66-Col.4/line11])*** ; "analyzing, by said module, the data portion according to a protocol that is associated with the physical communication port, ***(authentication/security and recognition functions by computer of the device [Col.4/lines 4-11]).***

Steinberg does not explicitly disclose "determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached, d. determining, by the module, based at least in part on said data portion analysis, whether to allow the data communication session, wherein if said data communication session is to be allowed, then transferring the one or more data portions with data stored in the associated buffer, if any exist, toward or from the physical communication port."

However, Mambakkam in an analogous art discloses an external mass storage device secured against unauthorized access that blocks access by disabling plug and play configurations if authentication is not successful ***(Mambakkam [abstract also see [Fig.8]).***

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Steinberg's secure storage device for transfer of data via removable storage with an external mass storage device secured against unauthorized access that blocks access by disabling plug and play configurations if authentication is not successful in order to provide additional security as suggested by

Mambakkam ***(Mambakkam [abstract also see [Fig.8]).***

Steinberg in view of Mambakkam does not explicitly disclose “and if said data communication session is not to be allowed, then modifying data transportation related to said data communication session, wherein if no decision may be reached on whether to allow, then storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for a next data portion, and if said decision may be reached , then proceeding proceed to step 'd';

However Hann in an analogous art discloses security communication system in which host security device intercepts and processes initial data packet information which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal. ***(Hann [Abstract/lines 11-18] also see buffer storage Hann [Col.10/lines 63-68]).***

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Steinberg’s secure storage device for transfer of data via removable storage with Mambakkam’s external mass storage device that secures against unauthorized access using a blocking technique with a security communication system in which host security device intercepts and processes initial data packet information which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal in order to provide additional security as suggested by Hann***(Hann[Abstract/lines 11-18] also see buffer storage***

Hann[Co1.11/lines 48-56]).

Regarding **claim 2** in view of claim 1, the references combined disclose "wherein the step of modifying the data transportation comprises blocking the transportation" ***(data is secured and only transferred if authentication has been successful Mambakkam [abstract also see block access [Fig.8/item 88])***

Regarding **claim 3** in view of claim 1, the references combined disclose "wherein the step of modifying the data transportation comprises modifying the type of the transportation", ***i.e. data transportation is modified by adding data to the image such as fingerprinting (Steinberg [Abstract] also see Steinberg[Fig.8]).***

Regarding **claim 4** in view of claim 1, the references combined disclose "wherein the step of modifying the data transportation comprises modifying a status of a requested file" ***i.e. data transportation is modified by adding data to the image such as fingerprinting (Steinberg [Abstract] also see Steinberg [Fig.8]).***

Regarding **claim 5** in view of claim 1, the references combined disclose "wherein the step of modifying the data transportation comprises correcting the data according to the communication protocol" ***i.e. data transportation is modified by adding data to the image such as fingerprinting (Steinberg [Abstract] also see Steinberg[Fig.8]).***

Regarding **claim 6**, in view of claim 1, the references combined disclose "wherein the physical communication port is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared"***(Steinberg[Fig.1] illustrates a secure storage device to physically engage with a PCMCIA card slot Steinberg[Col.4/lines 32-37]).***

Regarding **claim 7**, in view of claim 1, the references combined disclose "wherein the physical communication port is a USB port" ***(see computer system bus using a USB, IEEE 1394, PCMCIA or other additional interface Mambakkam [abstract]).***

Regarding **claim 8**, in view of claim 1, the references combined disclose "wherein the physical communication port is wireless" ***(see computer system bus using a USB, idée 1394, PCMCIA or other additional interface Mambakkam[abstract]).***

Regarding **claim 9**, in view of claim 1, the references combined disclose "wherein the step of analyzing the data portion further comprising: (i) determining whether additional processing based on a higher level protocol is required", wherein if additional processing is not required, then continuing at step 'c', otherwise -continuing at step (ii); and (ii) processing part of the data portion relevant to the higher level protocol according to the higher level protocol and returning to step (i)", ***i.e. using a security function, the device processes authentication data and original data and encrypts where the system may require additional level of protocol by requesting a password key for decryption and further requiring the computer to verify authentication data of questionable authenticity ([Steinberg[Abstract]).***

Regarding **claim 10**, in view of claim 9, the references combined disclose "wherein the step of analyzing the data portion comprises analyzing relevant to a higher level protocol that is associated with the external device" ***i.e. using a security function, the device processes authentication data and original data and encrypts***

where the system may require additional level of protocol by requesting a password key for decryption and further requiring the computer to verify authentication data of questionable authenticity ([Steinberg[Abstract]).

Regarding **claim 11**, in view of claim 10, the references combined disclose “wherein the data communication session is associated with an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols” ***(see computer system bus using a USB, iEEE 1394, PCMCIA or other additional interface Mambakkam [abstract]).***

Regarding **claim 12**, in view of claim 1, the references combined disclose “wherein the step of analyzing the data portion is performed in respect of the data stored in the associated buffer” ***(host security device intercepts and process initial data packet information containing user authorization information which is stored from buffer Hann [Abstract/lines 11-18] see buffer storage Hann [Co1.11/lines 48-56]).***

Regarding **claim 13**, in view of claim 1, the references combined disclose “wherein the step of determining whether a decision on the data communication session may be reached is performed in respect of the data stored in the associated buffer” ***(host security device intercepts and process initial data packet information containing user authorization information which is stored from buffer Hann [Abstract/lines 11-18] see buffer storage Hann [Co1.11/lines 48-56]).***

Regarding **claim 14**, in view of claim 1, the references combined disclose "wherein the step of determining whether to allow the data communication session is performed in respect of the data stored in the associated buffer" ***(host security device intercepts and process initial data packet information containing user authorization information which is stored from buffer Hann [Abstract/lines 11-18] see buffer storage Hann [Co1.11/lines 48-56]).***

Regarding **claim 15**, in view of claim 1, the references combined disclose "wherein the step of receiving a data portion comprises receiving a data portion selected from a group consisting of packet and SCSI block" ***(host security device intercepts and process initial data packet information containing user authorization information Hann [Abstract/lines 11-18]).***

Regarding **claim 16** in view of claim 1, the references combined disclose "wherein the step of receiving the data portion comprises obtaining the data portion by emulating a class driver" ***(Filtering device allows files with certain extensions to be secured Steinberg [Fig.10/item 170 &172] also see Steinberg[Col.8 line 59-67]).***

Regarding **claim 17**, in view of claim 1, the references combined disclose "wherein step of receiving the data portion comprises obtaining the data portion by emulating a filter module", i.e. imitating a filter device which accepts a certain type of data as input, transforms it in some manner, and then outputs the transformed data" ***(Filtering device allows files with certain extensions to be secured Steinberg [Fig.10/item 170 &172] also see Steinberg [Col.8 line 59-67]).***

Regarding **claim 18**, in view of claim 1, the references combined disclose "wherein the step of analyzing the data portion according to a protocol associated with the physical communication port further comprises: parsing the data portion; reassembling the data; analyzing the reassembled data" ***(Filtering device Steinberg [Fig.10/item 170 &172] also see Steinberg[Col.8 line 59-67]).***

Regarding **claim 19**, in view of claim 1, the references combined disclose "wherein the step of determining whether to allow the communication session comprises reviewing a security policy" ***(authentication/security and recognition functions by computer of the device Steinberg [Col.4/lines 4-11]).***

Regarding **claim 20**, in view of claim 1, the references combined disclose "wherein the step of determining whether to allow the communication session comprises examining the working environment in which the computer is operating and allowing the communication only if said computer is operating in one or more of certain working environments" ***(access is denied by disabling plug and play configurations if authentication is not successful (Mambakkam [abstract also see [Fig.8]).***

Regarding **claim 35**, in view of claim 10, the references combined disclose "wherein the device is a device selected from a group of devices consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle" ***(see computer system bus using a USB, iEEE 1394, PCMCIA or other additional interface Mambakkam [abstract]).***

Regarding **claim 37** in view of claim 1, the references combined disclose "wherein determining whether to allow the data communication session is based on a plurality of data portions wherein at least one of said plurality of data portions is stored in said buffer" ***(Data control information is stored in buffer storage Hann [Col.10/lines 63-68]).***

7. **Claims 1-15, and 17-35** are rejected under 35 U.S.C. 103(a) as being unpatentable over Patent Number: 6,134,591 to Nickles, in view of Patent Number: 4,799,153 to Hann et al (hereafter referenced as Hann)

Regarding **claim 21**, Nickles discloses "a system for enhancing the security of a private network being accessed by a computer" ***(security server protects network resources and information [Abstract/ lines 3-10]),*** "the system comprising: a client agent installed on a computer the client agent having an associated security policy" ***(see Client agent[Fig.1/item 16] connected to network[Fig.1/item14] which interconnects with a security server allowing connection to private network [Fig.1/item12])***; "a security manager communicatively coupled to the private network ; wherein the client agent is being operative to: detect a data transfer between a hardware device connected to the computer through a physical communication port of the computer" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios and options the server can utilize Nickles[Col.12/lines 15-26])***; Nickles does not explicitly disclose "analyze the data transfer according to a communication protocol associated with the physical communication port; and verify whether the data transfer is allowable based on the analysis of the data and the security policy; and wherein the security manager is being operable to associate a security policy with the client agent"

However Hann in an analogous art discloses security communication system in which host security device intercepts and processes/analyzes initial data packet information which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal. ***(Hann [Abstract/lines 11-18] also see buffer storage Hann [Co1.11/lines 48-56]).***

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Nickles network security integration method and system with a security communication system in which host security device intercepts and processes initial data packet information which is stored within buffer storage located between the I/O channel to determine user authentication and identity to thereby establish a communication session between user and terminal in order to provide additional security as suggested by Hann***(Hann[Abstract/lines 11-18] also see buffer storage Hann[Co1.11/lines 48-56]).***

Regarding **claim 22**, in view of claim 21, the references combined disclose "wherein the security manager is operable to verify that the security policy is correct" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios and options the server can utilize when verifying Nickles[Col.12/lines 15-26]).***

Regarding **claim 23**, in view of claim 21, the references combined disclose "wherein the security policy includes a plurality of rules that at least define limits on data transfers during a communication session***" (utilizing the object manager, security server reviews transaction table database information which contains different scenarios, rules and options the server can utilize when verifying Nickles [Col.12/lines 15-26]).***

Regarding **claim 24**, in view of claim 21, the references combined disclose "wherein the security policy includes a plurality of rules that at least define the type of operations that can be performed during a communication session" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios, rules and options the server can utilize when verifying Nickles [Col.12/lines 15-26]).***

Regarding **claim 25**, in view of claim 21, the references combined disclose "wherein the security manager is operable to disable any communication with the computer unless the client agent associated with the computer is active" ***(Nickles[Fig.12B/item 1232 user's transaction is aborted if password is invalid also see Nickles[Col.19/ lines 50-54]).***

Regarding **claim 26**, in view of claim 21, the references combined disclose "wherein the physical communication ports is selected from a group consisting of SCSI bus, Serial, Parallel, FireWire, PCMCIA bus, cellular, fiber channel, Bluetooth, iSCSI, Infiniband, and Infrared" ***(see computer system bus and I/O port interface Nickles[Fig.4/items 84 & 85] also see Nickles[Col.9/lines1-2]).***

Regarding **claim 27**, in view of claim 21, the references combined disclose "wherein the physical communication ports are a USB port" ***(see computer system bus and I/O port interface Nickles [Fig.4/items 84 & 85] also see Nickles [Col.9/lines1-2]).***

Regarding **claim 28**, in view of claim 21, the references combined disclose "wherein the physical communication port is wireless" ***(see computer system bus and I/O port interface Nickles [Fig.4/items 84 & 85] also see Nickles [Col.9/lines1-2]).***

Regarding **claim 29**, in view of claim 21, the references combined disclose "wherein the client agent is associated with the security policy by loading the security policy into the client agent", ***(within tables used by object manager is contained a user table which specifies which users have access and works with an associated network protocol loaded on clients computer such as HTTP, FTP, e-mail and TELNET Nickles [Col.13/lines 60-67] also see user tables Nickles [Col.12/ lines26-30]).***

Regarding **claim 30**, in view of claim 21, the references combined disclose "wherein the security manager is operable to verify that the security policy loaded into the client agent has not been modified" ***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios, rules and options the server can utilize when verifying Nickles [Col.12/lines 15-26]).***

Regarding **claim 31** in view of claim 21, the references combined disclose "wherein the client agent is further operative to transmit a report to the a security server, the report identifying events that occurred with the computer in view of the security policy" ***(client computer transmits log data to security server specifying where to log data of systems Nickles [Col.15/lines 9-22]).***

Regarding **claim 32** in view of claim 21, the references combined disclose "wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with the hardware device, wherein the hardware device is selected from a group consisting of flash memory, removable hard disk drive, floppy disk, writable CD ROM, a PDA, a cellular phone, a WiFi dongle and a Bluetooth dongle" ***(authorization functions are performed in conjunction with tables which specify the different levels of authorization Nickles[Col.6/lines 7-16], each device or computer connected to network is assigned a unique code which corresponds to table Nickles[Col.7/ lines20-21]).***

Regarding **claim 33**, in view of claim 21, the references combined disclose "wherein the client agent is operable to analyze the data based on a higher level protocol that is associated with an application selected from a group consisting of synchronization applications for PDA, Java applications for synchronization with cellular phone, backup storage applications, Bluetooth and WiFi protocols" ***(authorization functions are performed in conjunction with tables which specify the different levels of authorization Nickles[Col.6/lines 7-16], each device or computer connected to network is assigned a unique code which corresponds to table Nickles[Col.7/ lines20-21]).***

Regarding **claim 34**, in view of claim 21, the references combined disclose " a computer having installed thereon a module software agent installed in a computer for enhancing the security of the computer" ***(security server protects network resources and information Nickles[Abstract/ lines 3-10])***, "the agent being operative to:
detect a data transfer passing through at least one physical communication
port of the computer"***(utilizing the object manager, security server reviews transaction table database information which contains different scenarios and options the server can utilize Nickles[Col.12/lines 15-26])***;
"analyze the data transfer according to a communication protocol associated with the at least one physical communication port; and verify the data transfer is allowable based on the analysis of the data and a security policy" ***(host security device intercepts and processes and if authorization is indicated a communication session between terminal and database processor is established Hann [Abstract/lines 11-18]).***

Regarding **claim 36**, in view of claim 21, the references combined disclose "wherein determining whether a decision on whether to allow the data communication session may be reached is based on a plurality of data portions, wherein at least one of said plurality of data portions is stored in said buffer" ***(Data control information is stored in buffer storage Hann [Col.10/lines 63-68]).***

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL ANDERSON whose telephone number is (571)270-5159. The examiner can normally be reached on Monday-Friday 8am til 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kieu-oanh(Krista) T. Bui can be reached on (571)272-7291. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KIEU-OANH BUI/	MICHAEL ANDERSON
Acting Supervisory Patent Examiner, Art Unit 2433	Examiner, Art Unit 2433